Q-106.167 - Versand von Spam-eMails über den DvISE-Server trotz Authentifizierung via »POP before SMTP«

Q-106.167 - Versand von Spam-eMails über den DvISE-Server trotz Authentifizierung via »POP before SMTP«

aus Tobit KB importiert - vom 16.09.2003 - Beitrag bei Tobit

Problem

Einige Aussenstellen sind via POP before SMTP an den DvISE-Server eingebunden. Der DvISE-Server ist nicht direkt an das Internet angebunden. Es ist ein eMail-Server oder eine Firewall zwischengeschaltet, die eingehende Nachrichten prüft und 1:1 an den DvISE Server weiterleitet.

Im DvISE PostMan ist als Einschränkung für das Weiterleiten der Punkt »POP3/IMAP4 Anmeldung erforderlich« aktiviert worden.

Allerdings wird der DvISE-Server dennoch also »Open Relay« eMail-Server für Spam-eMails missbraucht.

Antwort

Die Einstellung »POP3/IMAP4 Anmeldung erforderlich« bewirkt, dass ein Weiterleiten nur dann möglich ist, wenn der Absender eines Forward-Jobs zuvor eine POP3- oder IMAP4-Anfrage durchgeführt hat, und somit eine Authentifizierung stattgefunden hat. Ohne eine solche Authentifizierung wird keine Weiterleitung durchgeführt.

Beim Abholvorgang der Aussenstelle muss die Kombination aus Benutzername und Passwort übermittelt werden, um auf das eigene Postfach Zugriff zu bekommen. Der DvISE-Server speichert die IP-Adresse des Requesters in seiner Datenbank. Wenn nun die Aussenstelle eine eMail zum Versenden an den DvISE-Server übermittelt, fragt dieser auf dem DvISE Mail Access Server nach der IP-Adresse. Bekommt dieser die IP-Adresse mit einem gültigen Status zurück, wird der Sendeauftrag angenommen. In der Standardkonfiguration des DvISE Mail Access Server werden Forward-Jobs ausschließlich innerhalb von zehn Minuten nach der letzten Authentifizierung ausgeführt. Danach ist eine erneute Authentifizierung erforderlich.

Ist der DvISE-Server nicht direkt an das Internet angebunden und Beispielsweise eine "ISA-Firewall" ist als Demilitarisierte Zone (DMZ) zur Sicherheit eingebaut worden, kann es zu Problemen kommen. Führt diese Firewall Beispielsweise eine Prüfung des Headers durch und leitet die Daten dann an den DvISE PostMan weiter, ist die Absende IP-Adresse immer die DMZ. Greift innerhalb der 10 Minuten jetzt ein Spam-Server auf ihr System zu, wird dieser als "Authentifiziert" vom DvISE PostMan akzeptiert und er leitet alle Anfragen automatisch weiter.

Um diesen Effekt zu beheben muss der DvISE PostMan die Daten entweder direkt von den Aussenstellen erhalten oder die Authentifizierungsmethode muss geändert werden. Weitere Informationen entnehmen Sie dem**KnowledgeBase Artikel Q-100.250**.

Hinweise:
Die Länge dieses Zeitraums, in der die IP-Adresse gespeichert wird, kann in der Datei MASERVER.INI aus dem Verzeichnis »DAVID\APPS\MASERVER\CODE« über den Parameter »AuthTimeWindow« frei definiert werden.